ComplyTec
ENTERPRISE COMPLIANCE

RSA Multi-Factor Authentication (MFA)

PRE-PLANNING GUIDE FOR Microsoft Office 365

As organizations move towards the cloud to deliver critical IT services the attack surface is expanding, and the perimeter is being disrupted.

Identity has become the most consequential attack vector with phishing and pretexting representing 81% of breaches according to the 2017 Verizon Data Breach Investigation Report.

Many would say that identity is the new perimeter. Considering this, it is no surprise that organizations are looking towards Multi-Factor Authentication (MFA) as a way of protecting against this reality.

Office 365 is often the gateway into the world of cloud services. It also offers more than the typical cloud application complexity when deciding on the best way to protect it with MFA. In fact, the strategy behind Office 365 architecture will likely dictate how other cloud services are secured and accessed.

There are a few things to be aware of when protecting Office 365.

Microsoft MFA for Office 365 and Microsoft Azure AD Premium

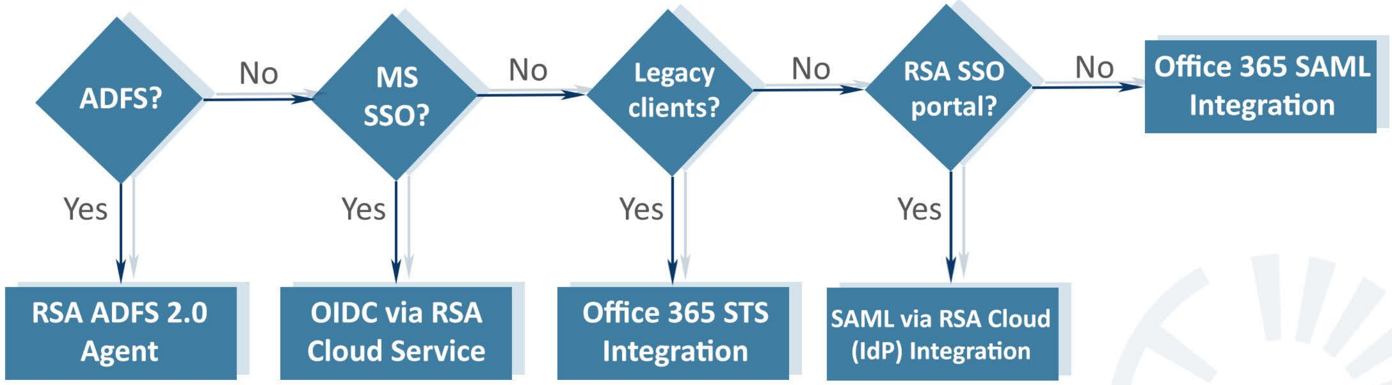
Microsoft offers MFA for Office 365 via Azure Active Directory Premium licenses. They also offer a subset of Azure MFA as part of an Office 365 subscription. The MFA included with an Office 365 subscription can only be used for Office 365 and not to protect other cloud applications or services. It does not support conditional policies, machine learning to evaluate risk, offline authentication and many other capabilities that would be expected in an enterprise MFA solution. Due to these limitations, it is probably adequate for smaller organizations who do not yet have other cloud applications to integrate with and have yet to define an overarching enterprise MFA strategy encompassing both and on-premise applications.

Organizations looking for an enterprise-ready MFA solution will look to Microsoft Azure AD Premium or to a third-party solution. Many of these companies have an existing investment in RSA MFA and can build out a comprehensive MFA strategy to leverage it.

RSA SecurID Access

The focus of the remainder of this paper is to walk through a decision process to determine the best method of protecting Office 365 in a specific environment using RSA SecurID Access. Many organizations are already using this solution to protect other resources such as virtual private network (VPN) access, Citrix, Windows and Linux/Unix or one of the other 400+ integrations and will need to determine how best to add this use case.

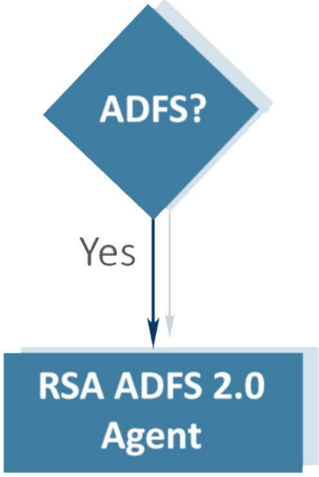
Below is a decision tree that ComplyTec has created to help guide you through this process:


ADFS?
No
MS SSO?
No
Legacy clients?
No
RSA SSO portal?
No
Office 365 SAML Integration
Yes
Yes
Yes
Yes
RSA ADFS 2.0 Agent
OIDC via RSA Cloud Service
Office 365 STS Integration
SAML via RSA Cloud (IdP) Integration

When choosing an MFA integration for Office 365 that works best for a given situation, there are a few things that need to be considered as illustrated in the graphic on the previus page.

The first is whether Active Directory Federation Services (ADFS) will be used to federate the on-premise Active Directory with Azure Active Directory.

When federating with ADFS, Azure Active Directory (the relying party) will rely on the on-premise Active Directory (the claims provider) for all authentication.



RSA ADFS 2.0 Agent

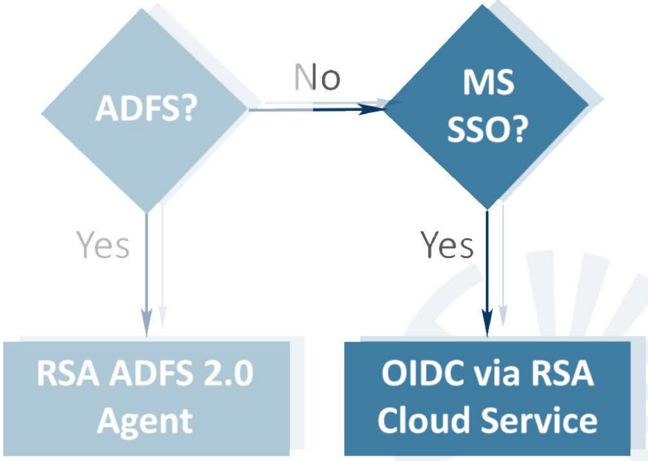
If using or planning to use ADFS as the identity strategy, the RSA ADFS 2.0 Agent for Authentication Manager is the integration to look at. It can be configured in two ways, either it can communicate with an on-premise RSA Authentication Manager appliance or directly to the RSA Cloud service via the REST API.

Once the RSA agent is registered with ADFS, it can be called on as required in the authentication policy. This allows continued use of Azure as the Single Sign-On (SSO) solution while providing strong identity assurance using RSA SecurID Access.

OIDC via RSA Cloud Service

When synchronizing the on-premise Active Directory with the Office 365 tenant via Azure AD Connect and not using Active Directory Federation Services (ADFS), the next decision is whether to use Azure Single Sign-On (SSO). If so, the OIDC via RSA Cloud Service integration is required.

When using the OIDC via RSA Cloud Service integration, Azure will manage primary authentication while using RSA to add additional authentication if called for by the triggered policy. A user will navigate to the Microsoft Access Panel or the Office 365 Portal to initiate the authentication sequence. Policies can be defined per application. This integration requires an Azure Active Directory Premium license on the Microsoft side.



Active Directory Authentication Libraries (ADAL)

In order to understand the remaining options for protecting Office 365 with MFA, a little background on Modern Authentication in needed. Modern Authentication is Microsoft's term for its implementation of the industry-standard OAuth 2.0 protocol. Microsoft implements this using Active Directory Authentication Libraries (ADAL).

Clients can be divided into two categories, active and passive. Older clients that use protocols like ActiveSync and Exchange Web Services to connect to Office 365 are considered active, while newer clients that connect to Office 365 using ADAL are considered passive. This distinction is because passive clients use an in-application browser control to provide the Azure AD sign-in experience instead of interacting directly with it. This allows support for MFA.

When choosing an integration with an MFA provider this is important, as active (also known as legacy) clients cannot be multi-factored and must be protected with other policies if support for them is required.

Microsoft has recently released a new feature in Azure Active Directory Conditional Access that that can prevent active authentication attempts, allowing Modern Authentication (ADAL) only.

Federating with SecurID Access

The remaining integration options allow office 365 to use RSA authentication to authenticate users using the on-premise Active Directory without relying on Active Directory Federation Services (ADFS). This is accomplished by federating the Azure tenant domain with the RSA infrastructure.

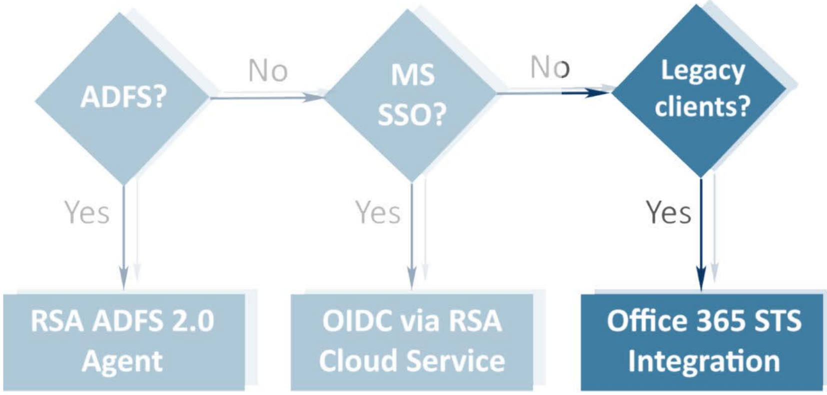
It is important to understand that federating an Azure Active Directory tenant with an RSA infrastructure is based on User Principal Name (UPN) suffixes and is not the same as federating using ADFS. It is essentially telling Azure Active Directory to rely on an identity provider, in this case the RSA infrastructure, to authenticate users. This is done with a few simple PowerShell commands and can be easily reversed. Synchronization of the on-premise Active Directory with Azure Active Directory using Azure AD Connect must still take place.

Depending on whether support for active (legacy) clients is required, this can be done in two ways:

- Security Token Service (STS) model using Web Services Federation (WS-Fed).
- SAML 2.0 based using Active Directory Authentication Libraries (ADAL).

Microsoft Office 365 STS Integration

If planning to support legacy clients use the Security Token Service (STS) model. This will support MFA for modern clients while allowing protection of legacy clients using policies based on location, user and other attributes.



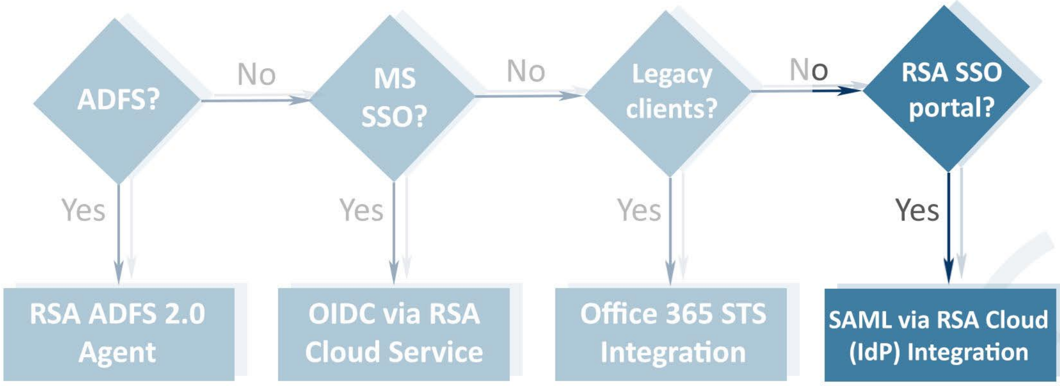
This integration also makes the RSA Single Sign-In (SSO) portal available. Users can either navigate to the RSA SSO portal or directly to Microsoft Office 365. In either case, they will be authenticated by the RSA solution before being granted access.

Microsoft Office 365 Integration (SAML)

When not planning to support legacy clients, use Active Directory Federation Service (ADFS), or use Microsoft Azure for SSO, the Microsoft Office 365 Integration using SAML 2.0 integration is a good fit.

It can be deployed in two ways depending on whether the RSA SSO portal will be used in the organization:

- SAML via RSA Cloud (IdP) integration
- Office 365 SAML integration

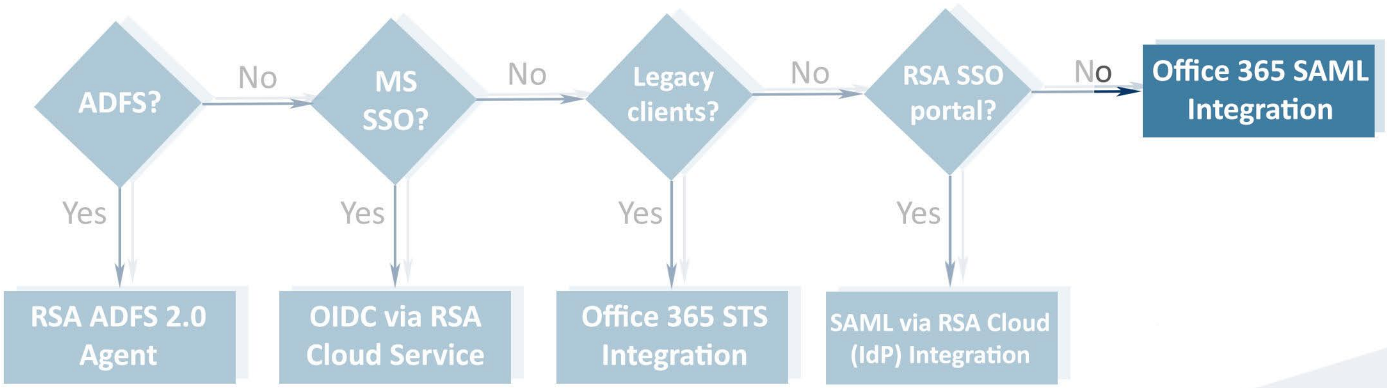

ADFS?
No
MS SSO?
No
Legacy clients?
No
RSA SSO portal?
Yes
Yes
Yes
Yes
RSA ADFS 2.0 Agent
OIDC via RSA Cloud Service
Office 365 STS Integration
SAML via RSA Cloud (IdP) Integration

SAML via RSA Cloud (IdP) Integration

The advantage of using the SAML via RSA Cloud (IdP) integration over the Office 365 SAML integration is that ports to allow access to the RSA SSO portal do not have to be opened, simplifying deployment if the portal is not required. Users will navigate to the Office 365 portal or authenticate directly via the client application. RSA SecurID will be called upon via the federation to provide for authentication.

Office 365 SAML Integration

When planning to use the RSA SSO portal, use the Office 365 SAML integration. Users can either navigate to the RSA SSO portal, navigate directly to the Microsoft Office 365 portal or authenticate via the client application itself. In either case, they will be authenticated by the RSA solution due to the federation before being granted access.


ADFS?
No
MS SSO?
No
Legacy clients?
No
RSA SSO portal?
No
Office 365 SAML Integration
Yes
Yes
Yes
Yes
RSA ADFS 2.0 Agent
OIDC via RSA Cloud Service
Office 365 STS Integration
SAML via RSA Cloud (IdP) Integration

If you would like to discuss how to secure employee access to office 365, please contact ComplyTec at sales@complytec.com or call us at (416) 410-5599 option 1.

www.complytec.com